UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,971	10/06/2003	Robert M. Best	493-37-3	4769

996 7590 02/09/2007

GRAYBEAL, JACKSON, HALEY LLP
155 - 108TH AVENUE NE
SUITE 350
BELLEVUE, WA 98004-5901

EXAMINER	
NGUYEN, KHOI	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/679,971	BEST, ROBERT M.	
	Examiner	Art Unit	
	Khoi Nguyen	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-89* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-89* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/01/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-89 are pending and considering for examination.

Claim Objections

2. The following phrases are objected to for lack of antecedent basis.

   a. "encrypted key", claim 11: line 1.

   b. "the portable game system", claim 12: lines 4-5.

   Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1, 11, 21 are rejected under 35 USC 112, second paragraph as being indefinite for failing to particularly point out and distinct claim the subject matter which applicant regards as the invention.

5. With regard to claim 1 on line 8, "first processor chip" is not clearly understood whether it is referring to a first semiconductor processor chip or another semiconductor processor chip. For the purpose of examining, first processor chip would be treated as first semiconductor processor chip.

6. With regard to claim 11 on line 1, "encrypted key" is not clearly understood whether it is referring to the encrypted session key, encrypted decryption key, or any other encryption key. For the purpose of examining, it will be considered as the encrypted session key.

7. With regard to claim 21 on line 7, "the processor chip" is not clearly understood whether it is referring to the cryptographic processor chip or an ordinary processor chip. For the purpose of examining, it will be considered as the cryptographic chip.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-12, 20-51, 58-76, and 83-89 are rejected under 35 USC 103(a) as being unpatentable over Eliott (US. Pat. No. 6712704), hereafter "Eliott" in view of, Ishibashi et al. (US Pat. No. 6728379) hereafter "Ishibashi",

10. With regard to claim 1, Eliott discloses a method of securely distributing game programs for execution in an electronic game system comprising the following steps:

(a) storing in a program storage medium a first game program (Fig. 1, Item 54, Fig. 11, Item 101, most servers would have contained a storage structure for data storage; thus it reads on storage medium) that is encrypted under control of an encryption key (Col. 3: line 10; Col. 25: lines 23-24; Col. 26: lines 28-30);

(b) a first semiconductor processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip)

(d) transferring (Col. 27: lines 54-57; Col. 25: lines 16-18, exchanging set of public key indicates transferring from the first processor to a second processor chip) from the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip) to a second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip);

(e) decrypting in the second processor chip (Col. 25: lines 30-31, decrypting session key at the video game system indicates decrypting in the second processor chip)

(f) decrypting in the second processor chip (Col. 25: lines 30-31, decrypting session key at the video game system indicates decrypting in the second processor chip) the encrypted game program (Col. 26: lines 32-34, downloaded game where the game is decrypted, indicates encrypted game program) under control of the decryption key (Col. 35: lines 6-8) to produce executable digital instructions stored in the second processor chip (Col. 33: lines 63-65, the game is ready to be executed indicates that executable digital instructions are produced); and

(g) executing the digital instructions in the second processor chip (Col. 3: lines 21-22; Col. 32: lines 40-47, issue to play the game reads on executing the digital instruction) to generate game data that specifies to the game system at least one variable characteristic of a player controlled object, wherein the executable digital instructions are inaccessible from the second processor chip (Fig. 1A, Item 86a and 86b)

However, Eliott does not disclose storing a decryption corresponding to the encryption key, encrypting the decryption key in the first processor chip to

produce an encrypted decryption key, transferring the encrypted decryption key, and decrypting the encrypted decryption key to reproduce the decryption key.

On the hand, Ishibashi discloses: storing a decryption key corresponding to the encryption key (Col. 2: lines 15-16), encrypting the decryption key in the first processor chip to produce an encrypted decryption key (Col. 2: lines 20-23), transferring the encrypted decryption key (Col. 2: lines 23-25), and decrypting the encrypted decryption key to reproduce the decryption key (Col. 2: lines 17-18).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

11. With regard to claim 21, Eliott discloses a cryptographic cartridge for protecting an encrypted program (abstract), the cartridge comprise:

a. A housing arranged for manual insertion into a game system (Fig. 1A, Item 54).

b. non-volatile data memory (Fig. 1, Item 76) and is inaccessible from the processor chip (Fig. 1A, Item 54, once the cartridge is removed from the

game console, there is not any communication between the cartridge and the game console at that time; thus indicates inaccessible)

However, Eliott does not disclose a cartridge comprises: a program storage medium in the housing storing the encrypted program; a cryptographic processor chip in the housing; non-volatile data memory in the processor chip for storing at least a first decryption key which is used to decrypt the encrypted program; decryption means in the processor chip to decrypt an input encrypted session key under control of a second decryption key to produce a decrypted session key; and encryption means in the processor chip to encrypt the first decryption key under control of the decrypted session key to produce an encrypted decryption key that is output

Nevertheless, Eliott discloses a system comprises:

c. A program storage medium in the housing storing the encrypted program (Fig. 11, Item 101; Col. 3: lines 10-11-11; Col. 25: lines 23-24; Col. 26: lines 28-30);

d. A cryptographic processor chip in the housing (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip)

e. decryption means in the processor chip (Col. 25: lines 30-31, decrypting session key at the video game system indicates decrypting in the processor chip) to decrypt an input encrypted session key to produce a decrypted session key (Col. 25: lines 27-31); and

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the program storage medium, a cryptographic processor that are housed in a cartridge for the game system, and decryption means in the processor chip as an integrally game unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

In addition, Eliott further does not disclose storing at least a first decryption key and which is used to decrypt the encrypted program; to decrypt an input encrypted session key under control of a second decryption key, and encryption means to encrypt the first decryption key under control of the decrypted session key to produce an encrypted decryption key that is output

Ishibashi, on the other hand, discloses storing at least a first decryption key and which is used to decrypt the encrypted program (Col. 2: lines 15-16);

to decrypt an input encrypted session key under control of a second decryption key (Col. 13: lines 19-20, being decrypted by a session key on the second processor indicates under control of a second decryption key) to produce a decrypted session key, and

encryption means in the processor chip to encrypt the first decryption key under control of the session key (Col. 7: lines 43-46) to produce an encrypted decryption key that is output.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

12. With regard to claim 27, Eliott discloses a cryptographic cartridge for protecting an encrypted program (abstract), the cartridge comprising:

a. a housing arranged for manual insertion into a game system (Fig. 1A, Item 54).;

However, Eliott does not disclose the cartridge comprising of a program storage medium in the housing that stores the encrypted program; a decryption key stored in encrypted form in the program storage medium for decrypting the

encrypted program; a crypto processor chip in the housing; and encryption means in the processor chip to encrypt the decryption key to produce an encrypted decryption key that is output from the housing.

Nevertheless, Eliott discloses a system comprising of:

b. a program storage medium in the housing that stores the encrypted program (Fig. 11, item 101; Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30) ;

c. decrypting the encrypted program (Fig. 11, Item 95).

d. a crypto processor chip in the housing (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip) and

However, Eliott does not discloses a decryption key stored in encrypted form, and encryption means in the processor chip to encrypt the decryption key to produce an encrypted decryption key that is output from the housing.

Ishibashi, on the other hand discloses a decryption key stored in encrypted form (Col. 10: lines 43-44); and encryption means in the processor chip to encrypt the decryption key to produce an encrypted decryption key (Col. 10: lines 43-44) that is output from the housing

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16)

13. With regard to claim 33, Eliott discloses a cryptographic system comprising a first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip) and a second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip) where a session key (Col. 25, line 27) is generated, encrypted (Col. 25, lines 27-31) and transferring the encrypted session key (Col. 25, lines 27-31).

Furthermore, Eliott discloses decrypting the encrypted session key (Col. 25, lines 27-31), decrypting encrypted key (Col. 25: lines 30-31), and executing the decrypted game program instructions (Col. 3: lines 21-22; Col. 32: lines 40-47).

In addition, Eliott discloses decrypting an encrypted game program (Col. 26: lines 32-34, downloaded game where the game is decrypted, indicates encrypted game program) under control of the decryption key (Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30; Col. 35: lines 6-8) to produce decrypted game

program instructions (Col. 33: lines 63-65, the game is ready to be executed indicates that executable digital instructions are produced).

However, Eliott does not disclose the first processor chip generating a session key; encrypting the session key; and transferring the encrypted session key to the second processor chip.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the first processor chip that generating a session key; encrypting the session key; and transferring the encrypted session key to the second processor chip as an integrally unit that represents an obvious manufacturing design choice of portability, data processing optimization, and economic benefits.

However, Eliott, also does not disclose of the first processor chip decrypting the encrypted decryption key under control of the session key to produce the game program decryption key. Also, Eliott does not disclose the second processor chip to store a game program decryption key, encrypting the game program decryption key under control of the decrypted session key; and transferring the encrypted decryption key to the first processor chip;

On the other hand, Ishibashi discloses decrypting the encrypted decryption key (Col. 2: lines 17-18) under control of the session key (Col. 7: lines 59-61) to produce the game program decryption key, to store a game program decryption key (Col. 2: lines 15-16); encrypting the game program decryption key (Col. 7: lines 43-46) under control of the decrypted session key (Col. 7: lines 59-61, session key is shared by both encryption/decryption process); and transferring the encrypted decryption key (Col. 2: lines 23-25)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16)

14. With regard to claim 35, Eliott discloses a method of securely distributing a game program for execution in an electronic game system (Abstract) comprising the following steps:

a. storing an encrypted game program in a program storage medium (Fig. 1, Item 54, Fig. 11, Item 101, most servers would have contained a storage structure for data storage; thus it reads on storage medium) in a first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor

processor chip), a portable housing (Fig. 1A, Item 54), and a unique identifier (Col. 3: lines 10-11, key unique to each hard drive reads on unique identifier).

b. encrypting the unique identifier in the first processor chip to produce an encrypted identifier (Fig. 11, Item 101, item "encrypted to Unique ID").

c. transmitting the encrypted identifier from the first processor chip through a data communications network (Fig. 11, item "telephone line"; Item "encrypted to Unique ID") to a server that supplied the encrypted game software (Col. 27: lines 34-37);

d. decrypting the encrypted identifier in the server to produce a decrypted identifier (Col. 29: lines 13-15, being able to identify the hard drive partition the unique ID of the hard drive must be in clear form to get to the drive and its partition so user can play the selected game; thus this reads on decrypting the encrypted identifier);

e. the decrypted identifier (Col. 29: lines 13-15, being able to identify the hard drive partition the unique ID of the hard drive must be in clear form to get to the drive and its partition so user can play the selected game; thus

this reads on decrypting the encrypted identifier) and encryption that produce at least one encrypted data block (Col. 29: lines 61-63);

f. decrypting in the electronic game system the encrypted data block (Fig. 11, Item 95, Col. 34, lines 45-46, decrypting on the fly indicates decrypting the encrypted data block) in a second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip); a unique identifier (Col. 3: lines 10-11, key unique to each hard drive reads on unique identifier) to produce a decrypted identifier (Col. 29: lines 13-15, being able to identify the hard drive partition the unique ID of the hard drive must be in clear form to get to the drive and its partition so user can play the selected game; thus this reads on decrypting the encrypted identifier), and a decrypted key (Fig. 11, Item 95, Item "Unique ID", the Unique ID is used to decrypt the encrypted data from the hard drive indicates a decrypted key).

g. decrypting the encrypted game program (Col. 26: lines 32-34, downloaded game where the game is decrypted, indicates encrypted game program) in the second processor chip under control of the decrypted key (Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30; Col. 35: lines 6-8) to produce executable digital instructions (Col. 33: lines 63-65, the game is ready to be executed indicates that executable digital instructions are

produced) if the decrypted identifier has a predetermined relationship with the unique identifier (Col. 26: lines 24-250).

However, Eliott does not disclose a second processor chip that contains the unique identifier and a decrypted key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to incorporate the unique identifier and a decrypted key in the second processor chip as an integrally unit that represents an obvious manufacturing design choice of portability, data processing optimization, and economic benefits.

Nevertheless, Eliott does not further disclose reencrypting in the server a digital key corresponding to the encrypted game.

Ishibashi, on the other hand, discloses reencrypting in the server a digital key corresponding to the encrypted game software (Col. 2: lines 20:23, encrypted content decryption key indicates a digital key corresponding to the encrypted game software).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of

encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16)

15. With regard to claim 59, Eliott discloses a cartridge comprising:

a. housing arranged for manual insertion into a game system (Fig. 1A, Item 54);

b. a program storage medium in the housing that stores the encrypted program (Fig. 11, item 101; Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30);

c. a decryption key for controlling decryption of the encrypted program (Fig. 11, Item 95, item "Unique ID" is used to decrypt the encrypted game program);

d. a crypto processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip);

e. a unique chip identifier (Col. 12: lines 36-37) in the crypto processor chip; and

f. encryption means in the crypto processor chip to encrypt the unique identifier to produce an encrypted identifier (Fig. 11, Item 101, item "encrypted to Unique ID").

However, Eliott does not disclose a cartridge comprises: a cryptographic processor chip in the housing, and encryption means in the crypto processor chip to encrypt the unique identifier to produce an encrypted identifier that is output from the housing.

Relatively, Eliott discloses a cryptographic processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip), encryption means in the crypto processor chip to encrypt the unique identifier to produce an encrypted identifier (Fig. 11, Item 101, item "encrypted to Unique ID"), and a housing (Fig. 1A, Item 54);

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to incorporate the cryptographic processor chip and encryption means in the crypto processor chip to encrypt the unique identifier to produce an encrypted identifier that is output from the housing as an integrally unit that represents an obvious manufacturing design choice of portability, data processing optimization, and economic benefits.

Furthermore, Eliott does not disclose a decryption key stored in encrypted form in the housing for controlling decryption of the encrypted program.

Ishibashi, on the other hand, discloses a decryption key stored in encrypted form (Col. 2: lines 20-23) .

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16)

16. With regard to claim 65, Eliott discloses a method of securely distributing game programs for execution in an electronic game system comprising the following steps:

a. storing in a program storage medium a first game program (Fig. 1, Item 54, Fig. 11, Item 101, most servers would have contained a storage structure for data storage; thus it reads on storage medium) that is encrypted under control of an encryption key (Col. 3: line 10; Col. 25: lines 23-24; Col. 26: lines 28-30);

b. a first semiconductor processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip)

c. transferring (Col. 27: lines 54-57; Col. 25: lines 16-18, exchanging set of public key indicates transferring from the first processor to a second processor chip) from the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip) to a second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip);

d. decrypting in the second processor chip (Col. 25: lines 30-31, decrypting session key at the video game system indicates decrypting in the second processor chip)

e. decrypting in the second processor chip (Col. 25: lines 30-31, decrypting session key at the video game system indicates decrypting in the second processor chip) the encrypted game program (Col. 26: lines 32-34, downloaded game where the game is decrypted, indicates encrypted game program) under control of the decryption key (Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30; Col. 35: lines 6-8) to produce executable digital instructions stored in the second processor chip (Col. 33: lines 63-65, the game is ready to be executed indicates that executable digital instructions are produced); and

f. executing the digital instructions in the second processor chip (Col. 3: lines 21-22; Col. 32: lines 40-47, issue to play the game reads on executing the digital instruction) to generate game data that specifies to the game system at least one variable characteristic of a player controlled object

However, Eliott does not disclose storing a decryption corresponding to the encryption key, encrypting the decryption key in the first processor chip to produce an encrypted decryption key, transferring the encrypted decryption key, and decrypting the encrypted decryption key to reproduce the decryption key.

On the hand, Ishibashi discloses: storing a decryption key corresponding to the encryption key (Col. 2: lines 15-16), encrypting the decryption key in the first processor chip to produce an encrypted decryption key (Col. 2: lines 20-23), transferring the encrypted decryption key (Col. 2: lines 23-25), and decrypting the encrypted decryption key to reproduce the decryption key (Col. 2: lines 17-18).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

17. With regard to claim 70, Eliott discloses a method of securely executing game program instructions in an electronic game system comprising a crypto processor chip and a co-processor (abstract), the method comprising the following steps:

a. storing in a program storage medium a game program (Fig. 1, Item 54, Fig. 11, Item 101, most servers would have contained a storage structure for data storage; thus it reads on storage medium) that is encrypted under control of an encryption key (Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30);

b. a non-volatile data memory (Fig. 4, Item 206, Hard drive indicates non-volatile read/write memory) in the crypto processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip);

c. decrypting the encrypted game program (Col. 26: lines 32-34, downloaded game where the game is decrypted, indicates encrypted game program) under control of the decryption key (Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30; Col. 35: lines 6-8) to produce executable digital instructions (Col. 33: lines 63-65, the game is ready to be executed indicates that executable digital instructions are produced); and

d. executing the digital instructions in a processor core in the crypto processor chip to generate game data (Fig. 4, Item 180, Fig. 2, Item 100) that is processed by a graphics co-processor (Fig. 2, Item 200) that generates graphics data for display on a display device.

However, Eliott does not disclose the decryption key and the executable digital instructions being inaccessible from the crypto processor chip.

Relatively, Eliott discloses a method that the decryption key and the executable digital instructions being inaccessible from the crypto processor chip (Fig. 1A, Item 54, the game cartridge that removably from the game console indicates being inaccessible from the crypto processor chip).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to incorporate this housing method as an integrally unit that represents an obvious manufacturing design choice of portability, data processing optimization, and economic benefits.

Furthermore, Eliott does not disclose storing a decryption key corresponding to the encryption key.

Ishibashi, on the other hand, discloses storing a decryption key corresponding to the encryption key (Col. 2: lines 15-16).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

18. With regard to claim 85, Eliott discloses a crypto processor chip for use in an electronic game system (Abstract), the chip comprising:

a. a non-volatile data memory (Fig. 4, Item 206, Item 182, Col. 11: lines 31-33).

b. decryption circuitry in the crypto processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip which include the decryption circuitry) for decrypting an externally stored encrypted game program (Col. 14: lines 10-14, Col. 27, lines 34-40) under control of the decryption key to produce a decrypted program of digital instructions (Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30; Col. 35: lines 6-8).

c. a data memory in the crypto processor chip for storing the decrypted program of digital instructions (Fig. 2, Item 300)

d. a processor core in the crypto processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip) for executing the digital instructions to generate game data (Col. 3: lines 21-22; Col. 32: lines 40-47, issue playing game indicates executing digital instruction which in turn generating game data); and

e. output circuitry in the crypto processor chip for outputting the game data (Col. 26: lines 32-34, the game is decrypted and executed indicates output of an crypto processor chip) for transmission from the crypto processor chip to a graphics co-processor chip that generates graphics data for display on a display device (Fig. 2, Item 100, 200, 144, and 58).

However, Eliott does not disclose a non-volatile data memory in the crypto processor chip and a data memory in the crypto processor chip for storing the decrypted program of digital instructions that is inaccessible from the crypto processor chip.

Relatively, Eliott discloses a non-volatile data memory (Fig. 4, Item 206, Item 182, Col. 11: lines 31-33) and a crypto processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, since server 101 performs encryption; thus it indicates a cryptographic processor chip.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to include a non-volatile data memory in a crypto processor chip to optimize game data communication which can result in better response from the game console.

Furthermore, Eliott does not disclose a non-volatile data memory in the processor chip for storing a decryption key.

Ishibashi, on the other hand, discloses a method for storing a decryption key (Col. 2: lines 15-16).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

19. With regard to claims 2 and 66, Eliott discloses the program storage medium (Fig. 1, Item 54, Fig. 11, Item 101, most servers would have contained a storage structure for data storage; thus it reads on storage medium), the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip), and a cartridge that is manually removable from the game system (Fig. 1A, item 54).

However, Eliott does not disclose the program storage medium and the first processor chip are housed in a cartridge that is manually removable from the game system.

Eliott, on the other hand, discloses a cartridge that is manually removable from the game system (Fig. 1A, Item 54).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the program storage medium and the first processor that are housed in a cartridge that is manually removable from the game system as an integrally game unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

20. With regard to claims 3 and 67, Eliott discloses the encryption key and the decryption key are one symmetric key (Col. 30: lines 8-12).

21. With regard to claims 4, 22, 28, 37, 60, 68, 73 Eliott discloses the program storage medium is a semiconductor memory (Fig. 2, Item 300; Col. 9: lines 23-25).

22. With regard to claims 5, 23, 29, 38, 61, 69, and 74 Eliott discloses the program storage medium is an optically readable disk (Col. 5: lines 22-24; Col. 11: lines 25-26; Col. 42: lines 15-17).

23. With regard to claims 6, 24, 30 and 43, Eliott discloses the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip) is connected to the game system (Fig. 11, Item "telephone line") during execution of at least some of the decrypted digital instructions (Col. 32: lines 40-43).

However, Eliott does not disclose the first processor chip is removably connected to the game system during execution of at least some of the decrypted digital instructions.

Nevertheless, Eliott discloses a removably game cartridge connected to the game system (Fig. 1A, Item 54).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the first processor chip that is removably from the game system as an integrally game unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

24. With regard to claims 7, 25, 31, and 44 Eliott discloses the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip) is connected to the game system (Fig. 11, Item "telephone line") during execution of at least some of the decrypted digital instructions (Col. 32: lines 40-43).

However, Eliott does not disclose the first processor chip is disconnected from the game system during execution of at least some of the decrypted digital instructions.

Nevertheless, Eliott discloses a game cartridge that disconnected from the game system (Fig. 1A, Item 54).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the first processor that is disconnected from the game system as an integrally game unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

25. With regard to claims 8, 45, 75, 88 Eliott discloses the second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip), but does not disclose the second processor chip is firmly attached to the game system.

Eliott, however, discloses a game cartridge that is firmly attached to the game system (Fig. 1A, item 54; Col.5: lines 27-31, inserted into the video game console in a secure position indicates that the cartridge was firmly situated).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the second processor chip that is firmly attached to the game system as an integrally game unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

26. With regard to claims 9, 46, 76, and 89 Eliott discloses the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip) and execution of the decrypted digital instructions (Col. 32: lines 40-43), but does not disclose the first processor chip is housed in a game cartridge that is removably connected to the game system during the decrypted digital instructions.

Eliott, however, discloses the first processor chip is housed in a game cartridge (Fig. 1A, Item 54) and removably attached to the game system (Fig. 1A, Item 54)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the first processor chip that is housed in a game cartridge and removably connected to the game system as an integrally video game storage unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

27. With regard to claims 10, Eliott discloses the further steps of securely distributing game programs for execution in an electronic game system comprising: of generating a session key (Col. 25: lines 28), the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would

most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip), and the second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip) but does not disclose generating a session key in the second processor chip.

However, Eliott discloses generating a session key in a processor chip (Col. 25: lines 27-31, DSP indicates a processor chip).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to include the step of generating a session key in the second processor as an integrally unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

Furthermore, Eliott does not disclose generating a session key in the second processor chip to control the encrypting of the decryption key in the first processor chip.

On the other hand, Ishibashi discloses generating a session key in the second processor chip to control the encrypting of the decryption key in the first

processor chip (Col. 5, lines 10-12, using the session key to encrypt the decryption key indicates control of the encrypting of the decryption key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

28. With regard to claims 11, 26, 48 Eliott discloses the encrypted **session** key (Col. 25, lines 28-31), the first processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on first semiconductor processor chip), and the second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates a second processor chip) but does not discloses the encrypted **session** key is transferred from the first processor chip to the second processor chip and a session key randomly generated in the second processor chip

However, Eliott discloses sets of public key are exchanged between processors (Col. 25: lines 16-18), a random number generator (Col. 34: lines 3-5), and communicate in encrypted form (Col. 25: lines 27-31)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to include the step of transferring the encrypted **session** key from the first processor chip to the second processor chip and a session key randomly generated in the second processor chip and communicate in encrypted form in order to provide a unique multilevel security system to combat privacy attacks and unscrupulous counterfeiters who produce and sell illegal game cartridges (Col. 1: lines 45-46).

Nevertheless, Eliott failed to disclose further, the encrypted **session** key is transferred from the first processor chip to the second processor chip under control of a session key.

Ishibashi, on the other hand, disclose the encrypted **session** key is transferred from the first processor chip to the second processor chip under control of a session key (Col. 5, lines 10-12, using the session key to encrypt the decryption key indicates control of the encrypting of the decryption key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

29. With regard to claims 12, 51, 84, Eliott discloses the player controlled object is an animated character (Fig. 1A, Item 60) with articulated appendages that are programmed to move in response to manual operation of at least one control device in the portable game system (Fig. 1A, item 86a and 86b).

30. With regard to claim 20, Eliott discloses at least some of the executable digital instructions (Col. 33: lines 63-65, the game is ready to be executed indicates that executable digital instructions). However, Eliott does not disclose at least some of the executable digital instructions are stored in the second processor chip in non-volatile read/write memory.

However, Eliott discloses a non-volatile read/write memory (Fig. 4, Item 206, Hard drive indicates non-volatile read/write memory).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to store at least some of the executable digital instructions in the second processor chip in non-volatile read/write memory to prolong the executable digital instructions for future use.

31. With regard to claim 32, Eliott disclose keys transferred (Col. 27: lines 54-57; Col. 25: lines 16-18, exchanging set of public key indicates transferring from the first

processor to a second processor chip) from the processor chip (Fig. 11, item 101, Col. 27: lines 35-26, 41-43, Internet servers and e-commerce server would most likely to contain at least 1 processor for data processing; thus it reads on processor chip) to a second crypto processor chip (Fig. 11, Item 95, being able to decrypt encrypted data indicates a crypto processor chip) but does not disclose encrypted decryption key is transferred.

Ishibashi, on the other hand, discloses encrypted decryption key is transferred (Col. 2: lines 23-25).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott to include key transferring method as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

32. With regard to claim 34, Eliott discloses the encrypted game program is stored in a program storage medium (Fig. 1, Item 54, Fig. 11, Item 101, most servers would have contained a storage structure for data storage; thus it reads on storage medium) that is encrypted under control of an encryption key; Col. 3: lines 10-11; Col. 25: lines 23-24; Col. 26: lines 28-30), the second processor chip (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console indicates

a second processor chip), and a game cartridge (Fig. 1A, Item 54) but does not disclose that it is housed with the second processor chip in a game cartridge.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to house the encrypted game program with the second processor chip in a game cartridge as an integrally unit that represents an obvious manufacturing design choice of portability, data processing optimization, and economic benefits.

33. With regard to claim 36, Eliott discloses the portable housing is a game memory cartridge that is manually removable from the electronic game system (Fig. 1A, Item 54).

34. With regard to claims 39, 40 Eliott discloses the data communications network comprises a retailer computer that stores the encrypted data block into a data storage medium (Col. 41-43) in the portable housing.

35. With regard to claim 41, Eliott discloses the decrypted identifier (Col. 29: lines 13-15, being able to identify the hard drive partition, the unique ID of the hard drive must be in clear form to get to the drive and its partition so user can play the selected game; thus this reads on decrypting the encrypted identifier) and the

same encrypted data block (Col. 37: lines 45-47, each chunk of data represents the same encrypted data block).

However, Eliott does not disclose the decrypted identifier together in the same encrypted data blocks.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the decrypted identifier in the same encrypted data blocks to optimize throughput through device communication synchronization.

Neverthelessr, Eliott does not further disclose the decrypted identifier and digital key are reencrypted together in the same encrypted data blocks.

Ishibashi, on the other hand, discloses reencrypting in the server a digital key corresponding to the encrypted game software (Col. 2: lines 20:23, encrypted content decryption key indicates a digital key corresponding to the encrypted game software).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott to include key

transferring method as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

36. With regard to claim 42, Eliott discloses the decrypted identifier (Col. 29: lines 13-15, being able to identify the hard drive partition, the unique ID of the hard drive must be in clear form to get to the drive and its partition so user can play the selected game; thus this reads on decrypting the encrypted identifier).

However, Eliott does not disclose the decrypted identifier and digital key are reencrypted in separate encrypted data blocks.

Relatively, Eliott discloses separate data blocks (Fig. 17A, item 508, Col. 38: lines 40-43, each chunk of data to be downloaded indicates separate data block)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the decrypted identifier and digital key in a separate encrypted data blocks to provide pervasive security in order to enhance the protection of data against data cryptanalysis.

Neverthelessr, Eliott does not further disclose the digital key are reencrypted

Ishibashi, on the other hand, discloses reencrypting in the server a digital key corresponding to the encrypted game software (Col. 2: lines 20:23, encrypted content decryption key indicates a digital key corresponding to the encrypted game software).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott to include key transferring method as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

37. With regard to claim 47, Eliott discloses the further steps of generating a session key (Col. 25: lines 28), the server (Fig. 11, item 101) but does not disclose generating a session key in the server.

However, Eliott discloses generating a session key in a processor chip (Col. 25: lines 27-31, DSP indicates a processor chip).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to generate the session key in the server as an obvious implementation of choice.

Furthermore, Eliott does not disclose generating a session key in the server to control the encrypting of the decryption key in the first processor chip.

On the other hand, Ishibashi discloses generating a session key in the second processor chip to control the encrypting of the decryption key in the first processor chip (Col. 5, lines 10-12, using the session key to encrypt the decryption key indicates control of the encrypting of the decryption key).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott by means of encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

38. With regard to claim 49, Eliott discloses at least some of the executable digital instructions are executed in a processor core in the second processor chip (Fig. 2, item 100, Col. 9: lines 33-34, video console which contains a cpu indicates second processor chip).

39. With regard to claims 50 and 83, Eliott discloses executing the digital instructions in the second processor chip (Col. 3: lines 21-22; Col. 32: lines 40-47, issue to play the game reads on executing the digital instruction) to generate game data that specifies to the game system at least one variable characteristic of a player

controlled object, wherein the executable digital instructions are inaccessible from the second processor chip (Fig. 1A, Item 86a and 86b).

40. With regard to claim 58, Eliott the game system further comprises a discrete display device for displaying the player controlled object moving in response to manual operation of at least one control device attached to the game system (Fig. 1A, Item 60).

41. With regard to claim 62, Eliott discloses the cartridge (Fig. 1A, Item 54) and decryption of the encrypted program in the game system (Col. 32: lines 40-43).

However, Eliott does not disclose the first processor chip is removably connected to the game system during execution of at least some of the decrypted digital instructions.

Nevertheless, Eliott discloses a removably game cartridge connected to the game system (Fig. 1A, Item 54).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to further modify the method of Eliott to implement the first processor chip that is removably from the game system as an

integrally game unit that represents an obvious manufacturing design choice of portability, data processing optimizing and economic benefits.

42. With regard to claim 63, Eliott discloses the cartridge is disconnected from the game system during execution of the program in the game system (Fig. 1A, Item 68)

43. With regard to claim 64, Eliott discloses the cartridge (Fig. 1A, Item 54), transfer encrypted key (Col. 27: lines 54-57; Col. 25: lines 16-18, exchanging set of public key indicates transferring from the first processor to a second processor chip) and a second crypto processor (Fig. 1A, Item 50; Fig. 2, Item 100, the CPU in the video game console that can perform decryption indicates a second crypto processor chip) in the game system.

However, Eliott does not disclose encrypted decryption key is transferred from the cartridge to chip in the game system.

On the other hand, Ishibashi, discloses the encrypted decryption key (Col. 2: lines 20-23).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Eliott by means of

encryption/decryption content data as taught by Ishibashi to prevent data from being leaked to a third party (Col. 1: line 16).

44. With regard to claims 71 and 86, Eliott discloses the game program is block encrypted (Col. 29: line 67) and the decrypting step block decrypts the block encrypted game program (Col. 30: line 10, since this is a symmetric encryption type, the same key would be used to decrypt the encrypted original block).

45. With regard to claims 72 and 87, Eliott discloses the encryption key and the decryption key are the same key for control of a symmetric encryption method (Col. 30: line 10, Two-fish is a symmetric encryption algorithm indicates that the same key is used).

46. Claims 13-18, 52-57, and 77-82 is rejected under 35 USC 103(a) as being unpatentable over Eliott in view of, Ishibashi further in view of Miyamoto et al. (US Pat. No. 6139433), hereafter "Miyamoto"

47. With regard to claims 13, 52, 77 neither Eliott nor Ishibashi discloses the game data specifies a location of an object in a simulated world.

However, Miyamoto discloses the game data specifies a location of an object in a simulated world (Fig. 11A, Item 829; Fig. 12, Item 836; Fig. 25A-C).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott and Ishibashi to incorporate the game data specifies a location of an object in a simulated world, as taught by Miyamoto to offer the user greater visual detail and maintain the users interest in the gaming device.

48. With regard to claims 14, 53, 78 neither Eliott nor Ishibashi discloses the game data specifies a location and an orientation of the player controlled object in a simulated world.

However, Miyamoto discloses the game data specifies a location (Fig. 11A, Item 829; Fig. 12, Item 836; Fig. 25A-C) and an orientation of the player controlled object in a simulated world (Fig. 27H).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott and Ishibashi to incorporate the game data specifies a location and an orientation of the player controlled object in a simulated world, as taught by Miyamoto to offer the user greater visual detail and maintain the users interest in the gaming device.

49. With regard to claims 15, 54, 79 neither Eliott nor Ishibashi discloses the game data specifies a movement direction of player controlled object in a simulated world.

However, Miyamoto discloses the game data specifies a movement direction of player controlled object in a simulated world (Fig. 27I and 27J).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott and Ishibashi to incorporate the game data specifies a movement direction of player controlled object in a simulated world, as taught by Miyamoto to offer the user greater visual detail and maintain the users interest in the gaming device.

50. With regard to claims 16, 55, 80 neither Eliott nor Ishibashi discloses the game data specifies a point of view location in a simulated world.

However, Miyamoto discloses the game data specifies a point of view location in a simulated world (Fig. 4C and 4D; Fig. 23D and 23E)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott and Ishibashi to incorporate the game data specifies a point of view location in a simulated world

as taught by Miyamoto to offer the user greater visual detail and maintain the users interest in the gaming device.

51. With regard to claims 17, 56, 81 neither Eliott nor Ishibashi discloses the game data specifies a location of a non-player object in a simulated world.

However, Miyamoto discloses the game data specifies a location of a non-player object in a simulated world (Fig. 4A-4F; Fig. 15C)

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott and Ishibashi to incorporate the game data specifies a location of a non-player object in a simulated world, as taught by Miyamoto to offer the user greater visual detail and maintain the users interest in the gaming device.

52. With regard to claims 18, 57, 82neither Eliott nor Ishibashi discloses the game data represents an image of at least a portion of a player controlled object.

However, Miyamoto discloses the game data represents an image of at least a portion of a player controlled object (Fig. 11C and 11D; Fig. 27E and 27F).

53. It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott and Ishibashi to incorporate the game data represents an image of at least a portion of a player controlled object, as taught by Miyamoto to offer the user greater visual detail and maintain the users interest in the gaming device.

54. Claim 19 is rejected under 35 USC 103(a) as being unpatentable over Eliott in view of, Ishibashi further in view of Miyamoto and further in view of Fujimoto et al. (US Pat. No. 6238291), hereafter "Fujimoto et al."

55. With regard to claim 19, neither Eliott nor Ishibashi nor Miyamoto discloses the game system comprises an LCD device.

However, Fujimoto discloses the game system comprises an LCD device (Fig. 1; Item 401).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the methods of Eliott, Ishibashi, and Miyamoto to incorporate an LCD device for the video game system, as taught by Fujimoto to offer the user greater visual detail in portable gaming environment and maintain the users interest in the gaming device.

Conclusion

56. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US Pat. No. 6884171 to Eck et al. (Discloses game distribution network with software emulation for hand-held video game such as Game Boy).

b. US Pat. No. 5632681 to Bakoglu et al. (Discloses game cartridge to request video frames).

c. US Pat. No. 6081785 to Oshima et al. (Discloses optical disk, manufacture process and cryptocommunication system and program license system).

d. US Pat. No. 6022274 to Takeda et al. (Discloses video game system with 3D graphic generating coprocessor).

e. US PGPub No. 2003/0177347 to Schneier et al. (Discloses authentication of computer generated game or test result).

f. US. PGPub No. 2001/0003714 to Kakata et al. (Discloses game program rewrite system suitable and aiming for construction of a game-on-demand system).

g. US Pat. No. 6544126 to Sawano et al. (Discloses portable hand-held console that can download and execute from other source).

h. US Pat. No. 7130425 to Strasser et al. (Discloses 2 separate processors to perform a bus-encryption for copy protection key).

i. US. PGPub No. 2002/0174351 to Jeong et al. (Discloses 2 crypto processors shared the same bus to perform encryption/decryption from each end of a communication system).

57. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est)
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen KN
Art Unit: 2132
Date:

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100